

Attorney Docket No. CLAR-00200

Request for First Extension of Time

Applicants hereby make a First Request for a First Extension of Time to extend the time for response from August 3, 2005 to September 6, 2005. The Commissioner is hereby authorized to charge any additional fees for this extension of time due or credit any overpayment to Deposit Account No. 50-2421.

Remarks:

This Amendment represents a sincere effort to respond to all of the issues raised in the Final Office Action of May 3, 2005, and to place the claims in condition for allowance or to reduce the issues for appeal.

Status of the Claims

Claims 1, 3-5, and 7-19 are the only pending claims.

In the Final Office Action of May 3, 2005, all of the claims were rejected under 35 USC 102 over U.S. Patent No. 6,557,029B2, of Szymansky et al. ("Szymansky") in view of U.S. Patent No. 6,363,482 to Shani ("Shani").

Final Office Action of May 3, 2005

All of the claims were rejected under 35 USC § 103(a) as being unpatentable over US Patent 6,557,029 to Szymansky ("Szymansky") in view of U.S. Patent 6,363,482 to Shani et al. The specific cited passages in Szymanski and Shani are shown below.

The References

U.S. Patent 6,557,029 to Szymansky et al. for System and Method for Distributing Messages describes a system and a method for real time message distribution from mobile users over a communication network. As described by Szymanski, mobile users enter information in handwritten form on a touch-sensitive screen using a stylus. The handwritten messages are converted into a graphics format and transmitted to a server. The server stores the graphic files in a database and transmits the graphic files to subscribers.

The passages in Szymanski that were relied upon in the Final Office Action are as follows:

"A preferred embodiment of the present invention uses hand-held computers with touch-sensitive screens. The information entered on the touch-sensitive screens is converted to graphic files. The graphic files are then transmitted to a computer server that is connected to the local area network of the subscribing firm. Computers that are connected by the local area network would display the handwritten information by using conventional Web browser software." (Column 2, lines 15-23)

"In the preferred embodiment, the data is transferred from the exchange's local area network to the subscribing firm's local area network using Simple Mail Transfer Protocol. However, various different publicly available or proprietary protocols could be used instead of Simple Mail Transfer Protocol" – (Column 3, lines 38-43)

"It is well known in the computer programming arts of techniques to insert information in a graphics file." (Column 3, lines 49 – 51)

"Market Look Manager 206 is responsible for the overall management and storage of information, user authentication and client profile information. The Market Look Manager 206 would perform client user authentication. Market Look Manager 206 would also route messages between EAN Interface Process 204 and HTTP Web Server 208.

Attorney Docket No. CLAR-00200

Market Look Manager 206 would also communicate with database 202 in which the graphic files representing the handwritten jottings and other information is stored.”

(Column 4, lines 11-18)

and Claim 11 *in toto*:

“11. The method of claim 1 wherein said network server provides subscriber management of transmissions of said network server further comprising the steps of:

tracking said transmissions comprising URLs;

checking said transmissions security status;

ascertaining said transmissions security of login;

transmitting said transmissions comprising requests for information from said user

further at least one of said transmissions comprising floor broker or securities booth digital signals;

selecting said transmissions comprising digital signals further comprising content comprising information as well as securities that said subscribing user selects;

transmitting said digital signals from said subscribing users of said network server monitors; and

displaying said transmissions.”

U.S. Patent 6,363,482 to Shani for Secure Broadband Communication describes a system for secure broadband communication. The system includes: (a) a server for transmitting data; and (b)

a client for receiving data. The client includes: (i) a public hardware identification key for data being sent to the server device, so that the client is identified by the public hardware identification key and the server device permits transmission to the client according to the public hardware identification key, and (ii) a private hardware identification key for controlling reception of data by the client. The private hardware identification key is known by the server, such that substantially only data being marked by the private identification key is passed to the client from the server. Note that control is at the server.

The one passage relied upon in the Final Office Action is

"However, such broadband network service, particularly through wireless networks, has added new problems. For example, wireless networks are potentially easily accessed by intruders, leaving data transmissions vulnerable to unauthorized interceptions. If two different networks are used for upstream and downstream communication, different types of hardware at the ISP must send and receive data, thereby requiring coordination between these types of hardware. Finally, transmitting data to a specific user is more complicated with broadband networks than with telephone networks, since data is broadcast to many users simultaneously so that the client device must select the correct data to be received. Thus, security and selectivity of reception of data are challenges for broadband networks and for the broadband modems used on these networks." (column 1, lines 35-40).

Applicants' Claimed Invention

According to the amended claims, a (wireless) device determines whether the signals received from the network are directed to the particular wireless device. If they are directed to the particular wireless device, the device screens the messages to determine whether they are configured under a proper protocol. This is to prevent unauthorized signal transmissions to the wireless device. If the messages are directed to the wireless device and are also configured under the proper protocol, then the system transmits authorized signals configured under the first protocol to the wireless device according to the first communication protocol.

The invention is directed to networks that are configured under a network protocol that requires all network devices that receive and send data packets related to administrative procedures within the network, such as device naming protocols. The invention prevents administrative communications from being transmitted to the wireless device, relieving the wireless device from the burdens of administrative data packets constantly being sent to the wireless device and requiring response, as well as the burdens of storing and processing such administrative data packets.

The gist of the invention is blocking these unwanted communications. This is variously claimed as:

"a filter mechanism configured manage data transmissions between the wireless device and the network device by filtering out data packets related to administrative device naming procedures within the network." (Claim 8)

"wherein the filter mechanism is configured to subsequently relay data packets that are sent by a network device that are configured according to the first protocol to the particular wireless device in response to the analyzer receiving a data packet sent by the particular wireless device to prevent data packets related to network renaming procedures from being sent to the wireless device." (Claim 9)

"wherein the filter mechanism is configured to subsequently relay data packets to the wireless device that are sent by a network device and that are configured according to the first protocol by preventing unnecessary data packet transmissions to the wireless device." (Claim 10)

"wherein the filter mechanism is configured to subsequently relay data packets that are sent by a network device that are configured according to the first protocol only to wireless devices that have transmitted such a packet having such indicia." (Claim 11)

"filter means for filtering our data transmissions between the wireless device and the network device upon a condition, where administrative renaming procedures are prevented from being transmitted to a wireless device." (Claim 12)

"wherein the filter means is configured to subsequently relay data packets that are sent by a network device and that are configured according to the first protocol to the particular wireless device in response to the examining means transmitting a data packet sent by the wireless device, wherein the examining

means prevents data packets related to network renaming procedures to the wireless device.” (Claim 13)

“wherein the filter means is configured to subsequently relay data packets to the wireless device that are sent by a network device and that are configured according to the first protocol, wherein the examining means prevents data packets related to network renaming procedures to the wireless device according to the first protocol.” (Claim 14)

“wherein the filter means is configured to subsequently relay data packets that are sent by a network device that are configured according to the first protocol only to wireless devices that have transmitted such a packet having such indicia, wherein the indicia alerts the examining means to prevent data packets related to network renaming procedures to the wireless device.” (Claim 15)

“a filter mechanism configured manage data transmissions between the wireless device and the network device and to prevent data packets related to network renaming procedures from being sent to the wireless device.” (Claim 16)

“wherein the filter mechanism is configured to subsequently relay data packets that are sent by a network device that are configured according to the first protocol that causes data packets related to network renaming procedures to be prevented from being sent to the particular wireless device.” (Claim 17)

“wherein the filter mechanism is configured to subsequently relay data packets to the wireless device that are sent by a network device and that are configured according to the first protocol that prevents data packets related to network renaming procedures from being sent to the wireless device.” (Claim 18)

“wherein the filter mechanism is configured to subsequently relay data packets that are sent by a network device that are configured according to the first protocol only to wireless devices that have transmitted such a packet having such indicia to prevent data packets related to network renaming procedures from being sent to the wireless device.” (Claim 19)

[Emphasis added.]

Discussion

Question: Whether claims reciting filtering means according to a protocol to block unwanted communications are allowable over the art of record.

Attorney Docket No. CLAR-00200

Unless the claimed elements are fully disclosed in the reference, it does not anticipate the invention. Furthermore, it is respectfully submitted that the details of the communication functions of the invention are not disclosed, suggested or otherwise "inherent" in either Szymansky or Shani et al..

Specifically, Szymanski's disclosure is directed to communications between LANs using SMTP, i.e.

"In the preferred embodiment, the data is transferred from the exchange's local area network to the subscribing firm's local area network using Simple Mail Transfer Protocol. However, various different publicly available or proprietary protocols could be used instead of Simple Mail Transfer Protocol" – (Column 3, lines 38-43)

To a Market Look Manager compliant server

"Market Look Manager 206 is responsible for the overall management and storage of information, user authentication and client profile information. The Market Look Manager 206 would perform client user authentication. Market Look Manager 206 would also route messages between EAN Interface Process 204 and HTTP Web Server 208. Market Look Manager 206 would also communicate with database 202 in which the graphic files representing the handwritten jottings and other information is stored." (Column 4, lines 11-18)

Market Look Manager, performs, *inter alia*, user authentication. However, this is not the filtering that is positively recited by Applicants.

Shani does not overcome the shortcomings of Szymansky. Instead, Shani describes a public key and private key system. , for example, at column 2, lines 9-25,

According to the teachings of the present invention there is provided a system for secure broadband communication, including: (a) a server device for transmitting data; and (b) a client device including a broadband modem for receiving data, the broadband modem including: (i) a public hardware identification key for being sent to the server device, such that the client device is identified by the public hardware identification key and such that the server device permits transmission to the client device through the broadband modem according to the public hardware identification key, and (ii) a private hardware identification key for controlling reception of data by the client device through the broadband modem, the private hardware identification key being known by the server

Attorney Docket No. CLAR-00200

device, such that substantially only data being marked by the private identification key is passed to the client device from the server device by the broadband modem.

The amendment is a proper Amendment After Final Action. The claims had been amended in previous amendments to include limitations directed to the prevention of transmission of administrative data packets to wireless devices, such as renaming protocols.

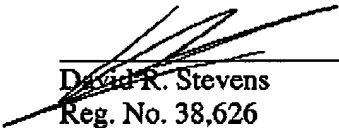
Applicant intends this as a genuine attempt to move the prosecution of this application forward.

Furthermore, Applicants submit that all of the claims as amended are in condition for allowance, and, accordingly, requests their allowance. If the Examiner finds that a telephone conference would expedite the prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Applicant hereby requests a one-month extension of time. The Commissioner is hereby authorized to charge this an any additional fees due or credit any overpayment to Deposit Account No. 50-2421.

Sincerely,

Dated: September 6, 2005


David R. Stevens
Reg. No. 38,626

Stevens Law Group
P.O. Box 1667
San Jose, CA 95109
Tel (408) 288-7588
Fax (408) 288-7542